Proje Adı: Sanallaştırılmış Sistemlerde Splunk ve Sysmon Kullanarak Tehdit Avcılığı ve SIEM Analitiği

Giriş:
Bu projede, sanal makine ortamında Splunk ve Sysmon kullanarak tehdit avcılığı ve SIEM (Güvenlik Bilgi ve Olay Yönetimi) analitiği gerçekleştirildi. Amaç, saldırgan hareketlerinin tespiti ve detaylı analizlerinin yapılmasıdır. Proje kapsamında, Kali Linux ve Windows 10 işletim sistemlerine sahip iki farklı sanal makine oluşturulmuştur. Kali Linux üzerinden saldırı operasyonları gerçekleştirilmiş, Windows 10 üzerinde ise Splunk ve Sysmon kullanılarak saldırıların izlenmesi ve analiz edilmesi sağlanmıştır.

Adımlar:

1. **Sanal Makine Kurulumu:**
    - VirtualBox kullanarak Kali Linux ve Windows 10 işletim sistemlerine sahip iki sanal makine oluşturuldu.
    - Kali Linux üzerinde Metasploit aracılığıyla saldırı senaryoları oluşturuldu.
2. **Metasploit Kullanımı:**
    - Kali Linux makinesinde msfvenom komutu ile zararlı yazılım oluşturuldu.
    - msfconsole komutu ile Metasploit framework'ü çalıştırıldı.
    - exploit komutları ile Windows 10 makinesindeki zafiyetler hedef alınarak saldırılar gerçekleştirildi.
3. **Splunk ve Sysmon Kurulumu:**
    - Windows 10 makinesine Splunk indirildi ve kuruldu.
    - Splunk üzerinden web arayüzü ile erişim sağlandı.
    - Sysmon, Windows 10 makinesine kuruldu. Sysmon, sistemdeki etkinlikleri izleyerek Windows Olay Günlüğü'ne detaylı kayıtlar düşüren bir sistem izleme aracıdır.
4. **Saldırıların İzlenmesi:**
    - Kali Linux üzerinden yapılan saldırılar Windows 10 makinesinde çalıştırıldı.
    - Sysmon ve Splunk entegrasyonu ile saldırı sonrası veriler toplandı.
    - Splunk üzerinde index=endpoint şeklinde sorgular yapılarak saldırı verileri analiz edildi.
    - Inputs.conf dosyası, Sysmon'un ürettiği verileri Splunk'a aktarmak için manipüle edildi.

5. **Sonuçlar:**
   Bu proje, sanal ortamda gerçekleştirilen saldırıların izlenmesi ve detaylı analizinin nasıl yapılabileceğini göstermektedir. Sysmon'un ürettiği sistem olaylarını Splunk aracılığıyla analiz ederek saldırganların hareketleri detaylı bir şekilde görüntülenmiştir. Böylece, bir tehdit avcılığı senaryosu başarıyla uygulanmıştır.

Mehmet Furkan KAPLAN

Cyber Security Analyst & Engineer

Project Title: Threat Hunting and SIEM Analytics Using Splunk and Sysmon in Virtualized Systems

Introduction:
In this project, threat hunting and SIEM (Security Information and Event Management) analytics were performed using Splunk and Sysmon within a virtual machine environment. The objective was to detect and analyze attacker activities in detail. Two virtual machines were created with Kali Linux and Windows 10 operating systems. Attacks were executed from Kali Linux, while the Windows 10 machine was monitored and analyzed using Splunk and Sysmon.

Steps:

1. **Virtual Machine Setup:**
    - Two virtual machines were created using VirtualBox: one with Kali Linux and another with Windows 10.
    - Metasploit operations were executed from the Kali Linux machine.
2. **Using Metasploit:**
    - A malicious file was created using the msfvenom command on the Kali Linux machine.
    - The msfconsole command was used to activate the Metasploit framework.
    - Vulnerabilities on the Windows 10 machine were exploited using the exploit command.
3. **Splunk and Sysmon Installation:**
    - Splunk was installed on the Windows 10 machine and accessed via the web interface.
    - Sysmon was installed on the Windows 10 machine. Sysmon is a system monitoring tool that tracks system events and logs them in the Windows Event Log.
4. **Monitoring Attacks:**
    - Attacks from Kali Linux were executed on the Windows 10 machine.
    - The integration of Sysmon and Splunk allowed for the collection of post-attack data.
    - The data were analyzed using queries such as index=endpoint in Splunk.
    - The inputs.conf file was configured to capture Sysmon-generated data in Splunk.

5. **Results:**
   This project demonstrated how to monitor and analyze attacks carried out in a virtual environment. System events generated by Sysmon were analyzed using Splunk, providing detailed insights into attacker activities. This scenario successfully showcased a practical threat hunting exercise.

Mehmet Furkan KAPLAN

Cyber Security Analyst & Engineer